	SC-402-Cryptography Paga No.: Dato:
	TOTTE COOTE S
	T1 0010011
	Tol-201901100 00 00 m. mm112-11 (2)
	Name-Shubham Patel
T17	Here (" & borne) = 100 p och
(1)	Here commended to a game
1	
(C.C.)	DC, + DC2 + DC3 + DC4 = D C4 = DC4 = X2+X3+X3
ė i	$\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 1$ $\rightarrow \alpha_5 = 1 + \alpha_1$
	$2C_3 + 2C_4 + 2C_5 + 2C_6 = 0$
W.CETT 1-	9C4+1 203+26+207=11-1= (207=1+203
	- Me board too 12 - 1
<u> </u>	So, we get,
	$3c, x_2 x_3 x_4 x_5 x_6 x_7$
	(0 0 10 10 10 10 10 10 10 10 10 10 10 10
	(0 0 10 10 910 910 0)
	(0 1 0 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
<u> </u>	"(60 mm) + (10-) (0-00 1 = 1 100 d 0)
	1 0 /hamol 1 0 mg (p + 2010 = 1 1)
	(1 1 0 0 0 0 1)
	(101m1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0
	trad = ('oc) d horn or the militial

	Propo No.: 2
[27 (a)	Assume $m 72$, Suppose 'a' is even; so a $2^{m-1} = 0 \pmod{2^m}$ colso o $2^{2m-2} = \pmod{2^m}$
200	Define $\alpha' = 3c + 2^{m-1}$ $mod 2^{m}$; $\frac{1}{2^{m}}$ $\frac{1}{30}$, $\frac{1}{100}$
(i	Suppose i'a' is odd. Define $x' = -x' - a$ $x = x - a$
	Then, $xe^t \pm xe$, and $h(xe^t) = h(xe^t)$

Page No.:_	(3)	_
Date :		

[3] Here we have, $\alpha = \alpha' \parallel c'$

Define $x' = x' \oplus x_0$, $x'' = x'' \oplus x_0$ $x'' = x'' \oplus x''$

Then x + x, and h(x) = h(x)

(H) (i), i = (con i id il con ind rid han)

Assigne une found a collison for he so he(x) = he(x') where x + x'.

le demote. (x=x, 11 x2 and x'=x, 11x2)

- Suppose that h(x) + h(α). Then h(α) 11 h(α) + h(α)11 h, (α).

And h, ch, cx) 11 Cho (x2) = ho (he (x2,1) 11

which coopered from Coopered the (xi)

- Therefore, we found collison for hi

1- The hicas) + hicocol), Then we have a

collison for hi.

By similar assumption, h(x) = h(x)and h(x) = h(x) because $x \neq x$. if follows $(x, x_2) \neq (x', x')$.

- We can always tound collison for hi, given collison for hz.

	Propo No.:
-	Dato:
(b)	Suppose coe forma de collison for
	his because hicoco = hicoco reshere
,	oc = oc'.
~ °C	mon on the man of the contraction
	Denote, x=x/1/02 and oc=x, 11 oco
	and the hope to the modern
_	Suppose that hi-1 (sc,) = hi-1 (sci)
	then hi-1 (oc) 11 hi-1 (oc) + hi-1 (oc) 11 hi-1 (oc)
***	and hichi-1(2,) 11 hi-1(x2) = h, (hi-1(x;'))
arit:	maille n hound no southi-(icoco)
- 73 1-	50 coefound collison for his
	Tf him (x2) + him (x2). Then coe have
	a collison for hi by similer -
	assumption à de considir con à
	Therefore coë i cun assume that
;	hi-1(00) = hi-1(00) and hi-1(00) - hi-1(00)
i i	because or ± or'. It follows or, ± or'
	Conside to ech morning and and acadille
_	collison for at least one of hi
0	collison tox at least one of hi
<i>p</i> ·	or hin, given collison for hi.
1	Carried or side mentages continued of the
4 1	to sammed (beside coosed home)